Crypto Template IKEv2-Vendor Payload Configuration Mode Commands

The Crypto Template IKEv2-Vendor Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for *ip-address-allocation*.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-vendor-payload)#
```

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

do show

Executes all **show** commands while in Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description `do show`

Usage Guidelines Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

⚠

Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `end`

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `exit`

Usage Guidelines Use this command to return to the parent configuration mode.

ignore-rekeying-requests

Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#
```

Syntax Description **`[ remove ] ignore-rekeying-requests`**

remove

If previously configured, removes the ignore-rekeying-requests configuration.

Usage Guidelines Prevents creation of a CHILD SA based on this crypto vendor template.

Example

The following command prevents creation of a CHILD SA based on this crypto vendor template:

`ignore-rekeying-requests`

ipsec

Configures the IPSec transform set to be used for this crypto template vendor payload.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#
```

Syntax Description **`ipsec transform-set list`** *`name`* **`[`***`name2`***`] [`***`name3`***`] [`***`name4`***`]`**

`remove ipsec transform-set list`

remove

Specifies the IPSec transform set to be deleted.

name

Specifies the context configured IPSec transform set name to be used in the crypto template vendor payload. This is a space-separated list. A maximum of 4 transform sets can be entered.

name must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines Use this command to list the IPSec transform set(s) to use in this crypto template vendor payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template vendor payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template vendor payload.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#
```

Syntax Description

```
lifetime { sec [ kilo-bytes kbytes ] | kilo-bytes kbytes | seqno sequence }

remove lifetime
```

remove

Removes the previously enabled lifetime configuration.

sec

sec must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this crypto template vendor payload.

kbytes must be an integer from 1 through 2147483647.

seqno *sequence*

Specifies lifetime in sequence number for IPSec Child Security Associations derived from this crypto vendor template.

sequence must be an integer from 10 through 4293918720.

Usage Guidelines Use this command to configure the number of seconds and/or kilobytes, or sequence number for IPSec Child Security Associations derived from this crypto template vendor payload.

Example

The following command configures the IPSec child SA lifetime to be *120* seconds:

```
lifetime 120
```

rekey

Configures IPSec Child Security Association rekeying.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#
```

Syntax Description

```
rekey [ keepalive ]
```

```
remove rekey
```

remove

Removes a previously enabled rekey configuration.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

Usage Guidelines Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the UE.

Example

The following command disables rekeying:

```
remove rekey
```